Association for Information Systems
AIS Electronic Library (AISeL)

WISP 2012 Proceedings

Pre-ICIS Workshop on Information Security and Privacy (SIGSEC)

Winter 12-14-2013

Cross-border M&A and Information Security Breaches: An Institutional Distance Perspective

Carol Hsu
Department of Information Management, National Taiwan University, carolhsu@ntu.edu.tw

Tawei Wang
University of Hawaii at Manoa

Cross-border M&A and Information Security Breaches: An Institutional Distance Perspective

Carol Hsu[1]
National Taiwan University, Taiwan

Tawei Wang
University of Hawaii at Manoa, USA

ABSTRACT

This research-in-progress paper examines the relation between information security breaches and cross-border mergers and acquisitions (M&A). Drawing from the institutional perspective, we use the concept of institutional distance to explain the impact of institutional differences on information security management at the transnational level. Using the secondary data collected from DataLossDB and SDC Platinum database, we empirically test the relation between institutional distances of two countries where the M&A firms register and the likelihood of information security breaches. The exploratory results indicate that institutional distance is positively associated with the likelihood of information security breaches. We conclude with theoretical implications and direction for further research.

Keywords: information security breaches, cross-border M&A, institutional theory.

INTRODUCTION

Growth in mergers and acquisitions (M&A) activities are becoming an important mechanism for companies to acquire new resources, diversify the risk and respond to changing market conditions. In responding to the globalization development and opportunities, the boundaries of M&A have been extended to cross-border context to allow multinational firms to

[1]Corresponding author: carolhsu@ntu.edu.tw

expand into foreign markets, gain access to local knowledge and foster international expansion (Xia 2011). The Bloomberg report on 2012 M&A Outlook indicates that global M&A activities show continuous growth and in the Americans region, cross-border deals accounted for 48.1% of total deal volume. Given this global trend, scholarly attention is emerging to analyze various benefits and risks associated with cross-border M&A deals.

In the literature, economic perspectives, such as transaction cost and resource-based theory, have been the dominant approach in understanding the strategic motivation and economic benefits of various cross-border alliance arrangements (Glaister et al. 1996; Xia 2011). Others have taken an institutional perspective to examine the quest of organizational legitimacy for resources obtainment (Kostova et al. 2002; Kostova et al. 1999). While these studies lay the theoretical foundation in analyzing cross-border M&A opportunities and formation, an emerging stream of literature are paying attention to the challenges and impact of inter-organizational differences on the survival of cross-border M&A. In particular, in the cross-border alliance context, studies have shown the implication of cultural differences, political influences and economic distance that might inhibit the alliance success (Barkema et al. 1997; Li et al. 1991; Tsang et al. 2007). Building on this stream of research, in this study, our objective is to explore whether such inter-organizational variation at the cross-country level would have another consequential impact of information security management.

Our theoretical rationale is that IS security literature has highlighted the importance of organizational culture, management policy and user behaviors in ensuring and maintaining good information security practices in organizations. Most prior studies focus on organizational level of analyses, scant attention is given to the inter-organizational context. We argue that in the context of cross-border M&A, the diversity of organizational practices, national culture and

regulation requirements situated in different institutional environments can lead to management difficulties and user conflicts with respect to the implementation and management of IS security requirements. Thus, the cross-country difference is an important variable that has the potential to enhance our understanding of inter-organizational information security management. To address this gap in research, we investigate the effect of institutional distance on the likelihood of information security breaches in the cross-border M&A context.

The organization of the paper is as follows. We present the theoretical framework and hypothesis development in the next section. The section that follows describes the research methodology and preliminary results. We conclude with discussion of the current findings and description of further research.

THEORETICAL BACKGROUND AND HYPOTHESIS DEVELOPMENT

In the examination of the cross-country differences, the traditional Hofstede paradigm has become the common choice and proxy of measurements in both IS and cross-border M&A. Although these studies have their merits in the contribution to the cross-culture research (Barkema et al. 1996; Kogut et al. 1998), others have criticized the shortcomings of Hofstede index to capture the complexity of institutional characteristics in different countries (Xia 2011; Xu et al. 2002). To address this problem, the concept of 'institutional distance' from the institutional perspective has emerged as an alternative approach to analyze cross-country differences (Kostova et al. 2002; Kostova et al. 1999). Institutional theorists argue that organizations need to confirm a set of institutional forces in order to gain organizational legitimacy for its survival in a given institutional environment. There are three forms of

institutional forces: the regulatory, the normative and the cognitive. The regulatory pillar represents the power and influence of the regulatory authority and legal system in ensuring compliance of organizational practices in an institutional setting (Scott 1995). The normative isomorphism refers to conformance of norms and standards that guides what organizations should or should not do, while the cognitive pillar focuses on the importance of cultural-cognitive elements embedded in a broader societal context.

Building on the institutional framework, institutional distance is defined as "the difference between the institutional profiles of the two countries" (p.316) (Kostova 1999). That is, the extent of dissimilarities of regulatory, normative and cognitive dimensions exists between two countries. This concept has been applied to the analysis of multinational enterprises (MNEs) operating in diverse institutional environments such as the study on foreign market entry, transfer of organizational practices, and governance strategies. These research works indicate that the larger the institutional distance, the more difficult the transfer or conversion of organizational practices across two countries (Kostova et al. 1999; Xu et al. 2002). This also applies to the situation of post-M&A integration, Shimizu et al. (2004) explain that "where the institutional distance (difference) between two countries is high, conflict between managers and employees of the two firms is likely to increase" (p.333). In our viewpoint, information security management is a form of organization practices required to be integrated and coordinated, we believe that the concept of institutional distance is applicable in explaining the possible conflicts and challenges associated with the management of information security issues in the context of cross-border M&A, as detailed below.

First, regulatory rules and requirements are typically country-specific. For instance, the U.S and the European Union have different regulatory approach to address the privacy issues

(Bellman et al. 2004). U.S adopts a more sector specific, i.e., public sector approach while the European Union opts for a more general inclusive approach. Empirical findings indicate the influence of national regulation on people's privacy concerns (Bellman et al. 2004; Milberg et al. 2000). Furthermore, compared with other countries, in the U.S, companies can make a decision to have voluntary disclosures concerning information security in their annual reports filed with the Securities and Exchange Commission (SEC) (Gordon et al. 2010). We argue that these differences in regulations and rules can be problematic in cross-border alliance context.

Second, the normative and cognitive dimensions of institutional profiles are related to the shared value, knowledge and culture in a society. Xu et al. (2002) argue that the normative distance is an important element for the transfer of organizational knowledge and skills between firms located in home and host country respectively. Kostova(1999) explains that the larger normative distance, the more difficult the transfer of organizational knowledge. The cognitive dimension is much related to the issue of national cultural differences. People from different countries vary in their interpretation of business practices and in risk tolerance. Studies have shown how the national cultures influence the managerial practices in managing post M&A integration process (Calori et al. 1994). In the case of information security management, the effect of national culture on users' security concerns and behaviors is also evident in the study by Dinev et al. (2009). In their study of protective technology use between the U.S and South Korea, their research results show the difference in the relation between subjective norm and behavioral intention between these two countries. They propose that the design of security policies and practices need to consider the cultural factors. Bellman et al. (2004) also offer the supporting evidence that cultural values have an effect on consumers' privacy concerns. In other words, we contend that in the situation of cross-border M&A, people would have diverse

attitudes towards information security issues such as sensitivity of data protection or attitudes towards protective information technologies. These differences will lead to conflicts in integrating or revising security policies at the post M&A stage.

Put together, our argument posits that the institutional distance derived from the dissimilarities in regulatory, normative, cognitive dimensions between countries can endanger the safeguard of information assets and soundness of information security management during the cross-alliance process. Thus, our research objective is to conduct an exploratory empirical study to test the following hypothesis

H1. *In a cross-border M&A context, the institutional distance between two countries are positively associated with the likelihood of information security breaches*.

METHODOLOGY

Sample

In order to test our hypothesis, we collected the following two sets of data: reported information security breaches and mergers and acquisitions.

We manually gathered reported information security breaches (denoted as BREACH) from DataLossDB (http://datalossdb.org) in the period from 2003 to 2013. DataLossDB collects reported information security breaches from news articles, blogs and websites on a daily basis. It also sends out inquiries to U.S. State departments for breach notification documents to identify security breaches. The sample period covered all the possible data point on DataLossDb. From this process, the initial sample consisted of 7,518 information security incidents. However, these

incidents included government agencies, non-for-profit organizations, and organizations that cannot be found in Compustat for firm characteristics. After excluding these firms/organizations, the resulting sample size was 1,553 information security events.

We then collected all mergers and acquisitions (M&A) activities from the SDC Platinum database. In order to understand the association between M&A and information security breaches in the context of institutional distance, we limit the M&A activities to have an acquirer in the United States and the target(s) in either Europe or Asian-Pacific countries. We considered the M&A activities starting from year 2000 (i.e., M&A activity can happen as early as three years before possible information security incidents). Since SDC Platinum database only has M&A data till 2012, our sampling period for alliances was from 2000 to 2012. This process resulted in 14,194 M&A activities. The year distribution of M&A activities (based on announcement dates) in our sample is given in Table 1. Table 1 demonstrates that there are more M&A activities in year 2000, 2007 and 2008.

Table 1.Year Distribution of M&As.

Year	# of Alliances	Year	# of Alliances	Year	# of Alliances
2000	1,617 (11.4%)	2005	1,060 (7.5%)	2010	846 (5.9%)
2001	1,233 (8.7%)	2006	1,106 (7.8%)	2011	1,052 (7.4%)
2002	876 (6.2%)	2007	1,452 (10.2%)	2012	831 (5.8%)
2003	888 (6.2%)	2008	1,497 (10.5%)		
2004	949 (6.7%)	2009	787 (5.5%)	Total	14,194 (100.0%)

Then we combined the information security events data with the M&A data. The final sample consisted of 14,194 observations. Among them, 221 observations were with information security breaches after the M&A activities while 13,973 observations were without. The number of M&A activities with security breaches in different year groups based on the date the breach

was reported in our sample is given in Table 2. Table 2 shows that there seem to be more M&A with security breaches in the year group from 2006 to 2008.

Table 2.Number of M&As with Security Breaches in Year Groups.

Year	# of Alliances with Breaches	Year	# of Alliances with Breaches
2003	2 (0.9%)	2009	14 (6.3%)
2004	1 (0.5%)	2010	20 (9.0%)
2005	10 (4.5%)	2011	28 (12.7%)
2006	25 (11.3%)	2012	28 (12.7%)
2007	53 (24.0%)		
2008	40 (18.1%)	Total	221 (100.0%)

Variables and Econometric Model

Our major variable of interest is the institutional distance as mentioned earlier. To capture the institutional distance, we considered the distance of the home countries of the acquirer (i.e., United States) in the M&A as in prior literature (Kostova et al. 2002; Kostova et al. 1999). Specifically, we assigned different numbers to different countries in the world based on the information given in the SDC database to show how far a country is from the United States which is the base case. We assigned zero for the targets in the United States in M&A arrangements. We set the targets in M&As in Europe as one, and Asia-Pacific Countries as two. Then we calculate the maximum difference (distance) in M&A as our distance measure (denoted as DISTANCE). For example, one M&A involved an acquirer from the United States and a target in Europe. The distance in this M&A activity is 1 which is the value for the variable DISTANCE.

Our preliminary model is given in Equation (1). Equation (1) was estimated by using logistic regression models with Huber-White corrected standard errors. In our preliminary model, we controlled for (1) the difference in size between the acquirer and the target which may

potentially affect the possibility of security breaches due to coordination issues (SIZEDIFF), and (2) the industry and year effects. We are still in the process of identifying other variables that may affect the likelihood of information security breaches in the context of cross-border M&A arrangements.

$$BREACH = \beta_0 + \beta_1 DISTANCE + \beta_1 SIZEDIFF + \Sigma\,\text{Industry} + \Sigma\,\text{Year} + \varepsilon \qquad (1)$$

Preliminary Results and Discussion

Our preliminary results are given in Table 3. There are three columns in Table 3. The first column presents the result based on full sample while the second and the third columns shows the results based on whether the information security breach was caused by outsiders or insiders. The results consistently show that institutional distance (DISTANCE) is positively associated with the likelihood of information security breaches. That is, the larger the institutional distance, the higher the possibility of information security breaches. In addition, the coefficient of DISTANCE is larger when the security breach is caused by insiders compared to outsiders. Our preliminary findings are consistent with our hypothesis. Specifically, the institutional distance of the participants in an M&A situation may result in differences in regulatory, normative, and cognitive aspects. Such difference can affect the effectiveness of information security management after the cross-border M&A which in turn increases the possibility of information security breaches. We consider this exploratory finding having several theoretical and practical implications. First, the result here contributes to the organizational and managerial aspects of IS security literature. As we point out earlier, previous studies have primary focus on intra-organizational issues. This result draws attention to the importance of information security

management at the inter-organizational level, in particular, in the context of cross-border M&A context. Second, this empirical study goes beyond the dominant Hofstede paradigm to examine transnational differences. Drawing from the institutional perspective, we introduce the significance of institutional distance in providing a more comprehensive picture of national differences. Third, our exploratory research hopes to stimulate more researches on other IS management issues related to strategic alliance. Given this is a growing organizational practices, we believe more researches can enhance the role and implication of information technology use in this particular context.

Table 3.Preliminary Results.

	Full Sample	**Breach Caused by Outsiders**	**Breach Caused by Insiders**
Intercept	-45.518***	-39.323***	-38.126
	(-12.32)	(-6.74)	(-3.99)
DISTANCE	0.632***	0.752***	0.766***
	(6.99)	(7.83)	(5.22)
SIZEDIFF	-0.000	-0.000	-0.000
	(-0.88)	(-0.80)	(-0.19)
Industry and Year Effect	Included	Included	Included
N	8,820	8,757	8,666
Pseudo R^2	0.08	0.07	0.08

* p< 0.10, ** p < 0.05, *** p < 0.01, z-statistics are given in parenthesis and are estimated with Huber-White standard errors. Industry effects are controlled but details are not reported.

REFERENCES

Barkema, H., and Bell, J. 1996. "Foreign Entry, Cultural Barriers, and Learning," Strategic Management Journal (17:2), pp 151-166.

Barkema, H., Shenkar, O., Vermeulen, F., and Bell, J. 1997. "Working Abroad, Working with Others: How Firms Learn to Operate International Joint Ventures," Academy of Management Journal (40:2), pp 426-442.

Bellman, S., Johnson, E., Kobrin, S., and Hohse, G. 2004."International Differences in Information Privacy Concern: A Global Survey of Consumers," Information Society (28:313-324).

Calori, R., Lubatkin, M., and Very, P. 1994."Control Mechanisms in Cross-border Acquisitions: An International Comparison," Organization Studies (15:3), pp 361-379.

Dinev, T., Goo, J., Hu, Q., and Nam, K. 2009. "User Behaviour Towards Protective Information Technologis: The Role of National Cultural Differences," Information Systems Journal (19:4), pp 391-412.

Glaister, K., and Buckley, P. 1996. "Strategic Motives for International Alliance Formation," Journal of Management Studies (33:3), pp 301-332.

Gordon, L. A., Loeb, M. P., and Sohail, T. 2010. "Market Value Of Voluntary Disclosures Concerning Information Security," MIS Quarterly (34:3), pp 567-594.

Kogut, B., and Singh, H. 1998. "The Effect of National Cultural on the Choice of Entry Mode," Journal of International Business Studies (19:3), pp 411-432.

Kostova, T. 1999. "Transnational Transfer of Strategic Organizational Practices: A Contextual Perspective," Academy of Management Review (24:2), pp 308-324.

Kostova, T., and Roth, K. 2002. "Adoption of an Organizational Practice by Subsidiaries of Multinational Corporations: Institutional and Relational Effects," Academy of Management Journal (45:1), pp 215-233.

Kostova, T., and Zaheer, S. 1999."Organizational Legitimacy under Conditons of Complexity: The Case of the Multinational Enterprise," academy of Management Review (24:1), pp 64-81.

Li, J., and Guisinger, S. 1991. "Comparative Business Failures of Foreign-Controlled Firms in the United States," Journal of International Business Studies (22:2), pp 209-224.

Milberg, S., Smith, J., and Burke, S. 2000. "Information Privacy: Coporate Management and National Regulation," Organisation Science (11:1), pp 35-57.

Scott, W. 1995. Institutions and Organizations, (Sage Publications: London.

Shimizu, K., Hitt, M., Vaidyanath, D., and Pisano, V. 2004. "Theoretical Foundations of Cross-Border Mergers and Acquisitions: A Review of Current Research and Recommendations for the Future," Journal of International Management (10:3), pp 307-353.

Tsang, E., and Yip, P. 2007. "Economic Distance and the Survival of Foreign Direct Investments," Academy of Management Journal (50:5), pp 1156-1168.

Xia, J. 2011. "Mutula Dependence, Partner Substitubility, and Repeated Partnership: The Survival of Cross-Border Alliances," Strategic Management Journal (32), pp 229-253.

Xu, D., and Shenkar, O. 2002. "Institutional Distance and the Multinational Enterprise," Academy of Management Review (27:4), pp 608-618.